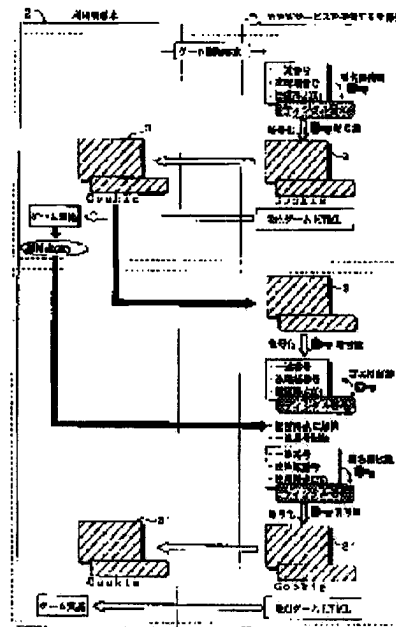


(11)Publication number : 11-098134
(43)Date of publication of application : 09.04.1999

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>
NTT ADVANCED TECHNOLOGY
CORP

(72)Inventor : KIKUCHI MITSUTAKA
ASANUMA TORU

SOLUTION: A computer 1 providing the WWW service that receives a service request from a user terminal 2 adds a series of or specific information to the Cookie and adds a digital signature to the information and encrypts the resulting information to conceal a data structure of the Cookie and sends it. Upon the receipt of the Cookie from a user terminal 2, it is decoded and the digital signature is extracted and it is authenticated. Furthermore, the unified relation between the served WWW service item and the user is confirmed by the series or specific information added to the Cookie.



[Date of request for examination]	24.04.2000
[Date of sending the examiner's decision of rejection]	09.03.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-98134

(43) 公開日 平成11年(1999) 4月9日

(51) Int.Cl. ⁸	識別記号	F I
H 0 4 L 9/32		H 0 4 L 9/00 6 7 5 B
G 0 6 F 13/00	3 5 7	G 0 6 F 13/00 3 5 7 Z
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00 6 1 0 C
	6 4 0	6 4 0 B

審査請求 未請求 請求項の数4 O L (全 8 頁)

(21) 出願番号 特願平9-258424

(22) 出願日 平成9年(1997) 9月24日

(71) 出願人 000004226

日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号

(71) 出願人 000102739

エヌ・ティ・ティ・アドバンステクノロジー株式会社
東京都武蔵野市御殿山1丁目1番3号

(72) 発明者 菊池 満孝

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74) 代理人 弁理士 小笠原 吉義 (外1名)

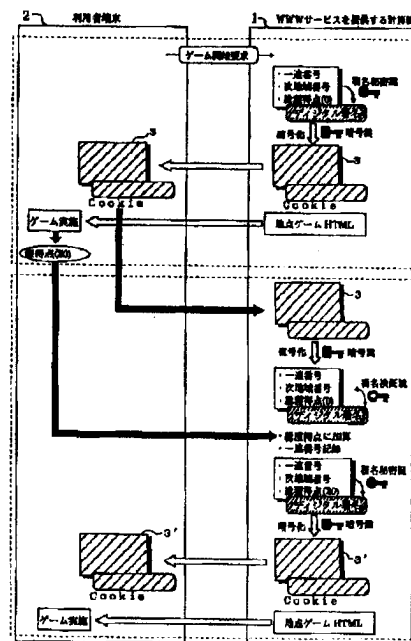
最終頁に続く

(54) 【発明の名称】 クッキーの改ざん・コピー検出処理方法およびプログラム記憶媒体

(57) 【要約】

【課題】 WWWサービス提供側でのCookieの改ざん検出、Cookieのコピー使用の検出を可能とし、Cookieの不正利用を防止してWWWサービスのセキュリティを維持する。

【解決手段】 WWWサービスを提供する計算機1は、利用者端末2からサービス要求があると、Cookieに一連または特定の情報を付加し、それにデジタル署名を付加して暗号化することにより、Cookieのデータ構造を隠蔽して送付する。利用者端末2からCookieを受信すると、それを復号し、デジタル署名を抽出して検証する。また、提供しているWWWサービス項目と利用者との関係の一意性を、Cookieに付加した一連または特定の情報によって確認する。



【特許請求の範囲】

【請求項1】 WWWサービスを提供する計算機で、クッキーを用いて利用者に提供するサービスの遷移の制御、サービス間でのデータの継承を行う方法において、クッキーに一連または特定の情報を付加する過程と、少なくとも前記一連または特定の情報を付加したクッキーのデータを暗号化して送付する過程と、前記暗号化したクッキーを受信したときにクッキーを復号する過程と、提供しているWWWサービス項目と利用者との関係の一意性を、前記クッキーに付加した一連または特定の情報によって確認する過程とを有し、WWWサービスのセキュリティを維持することを特徴とするクッキーの改ざん・コピー検出処理方法。

【請求項2】 WWWサービスを提供する計算機で、クッキーを用いて利用者に提供するサービスの遷移の制御、サービス間でのデータの継承を行う方法において、クッキーに一連または特定の情報を付加する過程と、前記一連または特定の情報を付加したクッキーにデジタル署名を付加する過程と、前記デジタル署名を付加したクッキーのデータを暗号化する過程と、暗号化したクッキーを送付する過程と、前記暗号化したクッキーを受信したときにクッキーを復号する過程と、復号したデータからデジタル署名を抽出し、デジタル署名を検証する過程と、提供しているWWWサービス項目と利用者との関係の一意性を、前記クッキーに付加した一連または特定の情報によって確認する過程とを有し、WWWサービスのセキュリティを維持することを特徴とするクッキーの改ざん・コピー検出処理方法。

【請求項3】 WWWサービスを提供する計算機で実行される、クッキーの改ざんまたはコピーによる不正利用を検出するためのプログラムを記憶したプログラム記憶媒体であって、クッキーに一連または特定の情報を付加する処理と、少なくとも前記一連または特定の情報を付加したクッキーのデータを暗号化して送付する処理と、前記暗号化したクッキーを受信したときにクッキーを復号する処理と、提供しているWWWサービス項目と利用者との関係の一意性を、前記クッキーに付加した一連または特定の情報によって確認する処理とを計算機に実行させるプログラムを格納したことを特徴とするプログラム記憶媒体。

【請求項4】 WWWサービスを提供する計算機で実行される、クッキーの改ざんまたはコピーによる不正利用を検出するためのプログラムを記憶したプログラム記憶媒体であって、クッキーに一連または特定の情報を付加する処理と、前記一連または特定の情報を付加したクッキーにデジタル署名を付加する処理と、前記デジタル署名を付加したクッキーのデータを暗号化する処理と、暗号化したクッキーを送付する処理と、前記暗号化したクッキーを受信したときにクッキーを復号する処理と、復号したデータからデジタル署名を抽出し、デ

ジタル署名を検証する処理と、提供しているWWWサービス項目と利用者との関係の一意性を、前記クッキーに付加した一連または特定の情報によって確認する処理とを計算機に実行させるプログラムを格納したことを特徴とするプログラム記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、クッキー（Cookie）の改ざんおよびコピーを、デジタル署名技術、暗号化技術、Cookieへの一連または特定の情報（番号）の付与により検出する方法およびそれを実現するためのプログラムを格納したプログラム記憶媒体に関する。

【0002】

【従来の技術】Cookieは、WWW（World Wide Web）サービスを提供する計算機であるWWWサーバが、利用者に提供するサービスの遷移の制御、サービス間でのデータの継承を行うために用いる情報であり、WWWブラウザがWWWサーバにアクセスした際にWWWサーバからWWWブラウザへ送付され、その後、WWWブラウザがWWWサーバにアクセスするときに、HTTPヘッダに埋め込まれてWWWサーバに転送されるようになっているものである。

【0003】従来、WWWサーバからWWWブラウザへ送付されたCookieは、利用者端末において、WWWブラウザの定める特定のファイルに記述され、端末利用者によって書き換えやコピーが可能であるため、WWWサーバは、受信したCookieが書き換えやコピーされたものであっても、それを検出することができなかった。

【0004】

【発明が解決しようとする課題】Cookieを用いて利用者のサービスの遷移を制御するWWWサービスの提供において、従来の方法では、利用者がCookieを書き換えることにより不正にWWWサービスを制御したり、利用者がCookieをコピーし、第三者に渡すかまたは第三者がネットワーク上でCookieをモニタすることにより入手したりして、不正にWWWサービスを利用することができるという問題がある。

【0005】本発明は、上記の問題点に鑑みてなされたもので、その目的とするところは、WWWサービス提供側でのCookieの改ざん検出、Cookieのコピー使用の検出を可能とし、Cookieの不正利用を防止してWWWサービスのセキュリティを維持する手段を提供することにある。

【0006】

【課題を解決するための手段】上記目的を達成するため、本発明は、Cookieにデジタル署名を付加することによるWWWサービス提供側でのCookieの改ざん検出、Cookieへの一連番号付与によるCo

okieのコピー使用の検出を可能とするもので、Cookieの暗号化と併せ、高いセキュリティを達成し得るようにするものである。具体的には、例えば次のように処理する。

【0007】WWWサービスを提供する計算機は、デジタル署名を作成するための署名秘密鍵とデジタル署名を検証するための署名検証鍵および暗号化のための秘密鍵を持ち、利用者端末から初期のサービス利用要求があったとき、利用者の次のサービス要求を決定する情報および唯一の一連番号、さらに利用者から入手したデータがあるときにはそのデータまたはその初期データを含むデータの集合に対し署名秘密鍵でデジタル署名を作成し、上記データの集合と共に暗号化の秘密鍵で暗号化し、Cookieとして利用者端末に送付する。

【0008】また、WWWサービスを提供する計算機は、利用者端末からサービス遷移要求があったとき、暗号化の秘密鍵を用いて受信したCookieを復号し、署名検証鍵を用いてデジタル署名を検証し、署名検証に失敗した場合には、利用者または第三者によるCookieの改ざんが行われたとみなしてサービスを直ちに停止する。署名検出に成功した場合には、正常なサービス遷移要求とみなし、利用者の次のサービス要求を制御するデータ、受信したCookieと同一の一連番号および利用者から入手したデータの集合に対し署名秘密鍵でデジタル署名を作成し、上記データの集合と共に暗号化の秘密鍵で暗号化し、Cookieとして利用者端末に送付する。

【0009】また、WWWサービスを提供する計算機は、利用者端末からサービス遷移要求があったとき、受信したCookieから入手した一連番号をサービス識別情報と共に記録し、これ以後、一つのサービス識別情報に対し2回以上同一の一連番号が記録されていれば、その一連のサービス遷移において第三者がCookieをコピーし不正利用が行われたとみなす。

【0010】特に、デジタル署名の作成および検証には、例えばESIGN (Efficientdigital SIGNature scheme) を用いると、高度なセキュリティを高速に実現することができる。また、暗号化および復号化には、例えば手順公開型の高速暗号化アルゴリズムであるFEAL (Fast data Encipherment ALgorithm) を用いると、高速処理が可能であるため望ましい。

【0011】以上の処理方法をコンピュータによって実現するためのプログラムは、コンピュータが読み取り可能な可搬媒体メモリ、半導体メモリ、ハードディスクなどの適当な記憶媒体に格納することができる。

【0012】

【発明の実施の形態】以下、図面を用いて本発明の具体的な実施の形態について説明する。図1は本発明を実施するシステムの構成例を示す。

【0013】図中、1はWWWサービスを提供する計算

機 (WWWサーバ)、11はWWWサービスのサービスプログラム、12は利用者のサービス要求に対してCookieに付与する一連番号を管理する一連番号管理部、13はCookieを生成するCookie生成部、14はCookieの改ざん・コピーが行われていないかどうかを検証するCookie検証部、15はCookieに付与するデジタル署名を作成および検証する署名作成・検証部、16はCookieの暗号化および復号化を行う暗号化・復号化部、17はHTTP (Hypertext Transfer Protocol) によるデータの送受信を制御するHTTPデーモン、18はCookieに付与する一連番号の最大値を記憶しておくための一連番号最大値管理ファイルを表す。

【0014】署名作成・検証部15が使用するデジタル署名作成用の署名秘密鍵とデジタル署名検証用の署名検証鍵、および暗号化・復号化部16が使用する暗号化用の暗号鍵は、計算機1のディスクまたはメモリ上に保持されている。

【0015】また、2はWWWサービスを利用する利用者端末、21はWWWサービスによって提供される情報の表示および入力を行うためのブラウザ、22はCookieを所定のファイル等へ書き込むCookie書き込み部、23はWWWサービスを提供する計算機1にCookieを通知するためにCookieを読み込むCookie読み込み部、24はCookieを保存する所定のファイル等のCookie格納部を表す。

【0016】Cookie書き込み部22およびCookie読み込み部23は、ブラウザ21に内蔵されている機能であり、ブラウザ21が、例えば米国Netscape Communications社が開発したNetscape Navigatorである場合、Cookieが格納されるCookie格納部24は「~Netscape\Navigator\Cookies.txt」のファイルである。また、ブラウザ21が、米国Microsoft社が開発したInternet Explorerの場合、Cookie格納部24は「\Windows\Cookies\XXX.txt」のファイルである。

【0017】図2は、本発明の一実施形態の作用を説明するための図である。本実施の形態では、WWWサービスを提供する計算機1は、いくつかの擬似的な地点を遷移しながらゲームが展開する形態の地点毎のゲームを、利用者端末2に提供するものとする。

【0018】利用者端末2からゲームの開始を要求すると、計算機1では、サービスプログラム11の制御のもとに、一連番号管理部12により一連番号最大値管理ファイル18を読み込んで、新規にこの要求のみに唯一な一連番号を付与し、次に行うゲームの地点識別子 (次地域番号) を決定し、総獲得点を初期設定する。次に、Cookieの生成にあたって、Cookie生成部13は署名作成・検証部15を呼び出し、一連番号、次地域

番号、総獲得点の3つのデータ集合に対し、E S I G Nの署名秘密鍵によりデジタル署名を作成し、さらに暗号化・復号化部16を呼び出して、F E A L暗号鍵によりそれらを暗号化し、C o o k i eを生成する。

【0019】なお、このC o o k i eのデジタル署名の作成および検証に用いるE S I G N (Efficient digital SIGNature scheme)については、参考文献として、例えば特開昭62-113191号公報、特開平01-147585号公報、特開平03-129384号公報がある。また、C o o k i eの暗号化および復号化に用いるF E A L (Fast data Encipherment ALgorithm)については、参考文献として、特開昭60-196059号公報、特開昭61-200778号公報がある。

【0020】以上のようにしてデジタル署名を付与して暗号化したC o o k i e 3を、当該地点のゲームを実行するHTMLファイルと共に、HTTPデーモン17を介して利用者端末2に送付する。

【0021】利用者端末2では、ブラウザ21によりHTMLファイルとC o o k i e 3を受信すると、C o o k i e書込み部22より、C o o k i e格納部24にC o o k i e 3を保存する。

【0022】次に、利用者端末2で利用者がゲームを実行し、次の地点のゲームを実行するため再び計算機1に要求を発行する際、C o o k i e読み部23によりC o o k i e格納部24からC o o k i e 3を読み出し、今回取得したゲームの獲得点とC o o k i e 3を計算機1へ送付する。

【0023】計算機1では、HTTPデーモン17を介して利用者端末2からのゲームの継続要求を受けると、サービスプログラム11は、C o o k i e検証部14を呼び出す。C o o k i e検証部14は、まず暗号化・復号化部16を呼び出してF E A L暗号鍵によりC o o k i eを復号する。その後、C o o k i e検証部14は、署名作成・検証部15を呼び出し、E S I G N署名検証鍵によりデジタル署名を検証する。

【0024】サービスプログラム11は、デジタル署名の検証に失敗したときには、C o o k i eが改ざんされたとみなして直ちにサービス続行を取り消す。検証に成功したときには、利用者端末2から送付された獲得点を総獲得点に加算し、次に行うゲームの地点識別子を決

定し、受信したC o o k i e 3から一連番号を抽出し、それらの3つのデータ集合に対し、署名作成・検証部15によってE S I G Nの署名秘密鍵によりデジタル署名を作成し、暗号化・復号化部16によりF E A L暗号鍵を用いて暗号化し、C o o k i e 3'を作成し、当該地点のゲームを実行するHTMLファイルと共に利用者

端末2に送付する。

【0025】上記の処理で受信したC o o k i e 3から抽出した一連番号は、ゲームの識別子と共に計算機1のディスクに記録し、以後、同一の一連番号とゲーム識別

子の組が複数回記録されていた場合には、C o o k i eの不正なコピーがなされたとみなす。

【0026】以上の実施の形態では、C o o k i eにより、利用者のゲーム実施地点の遷移と総獲得点の記録を計算機1の完全主導で制御することで正常な実施が成り立っており、利用者によるゲーム実施地点および総獲得点の改ざんを、デジタル署名を付加することにより計算機1で検出可能としている。

【0027】なお、利用者端末2でゲームを実施した結果のゲームの獲得点は、C o o k i e 3とは別に計算機1へ送付する。利用者端末2では、C o o k i e 3を保存するのみで暗号化・復号化を含め、一切の加工は行わない。例えば、本実施の形態におけるゲームの場合、W W Wサーバからダウンロードするゲームプログラム内で点数をスクランブルすることにより、利用者端末2におけるゲーム点数の改ざんを防止しているが、これはC o o k i eの改ざん防止とは独立しており、直接的に関係する事項ではない。

【0028】図3は、図1に示すサービスプログラム11の処理フローチャートである。ステップS1では、利用者端末2からの要求に対し、初期アクセスかどうかを判定し、新たにゲームを開始することを要求する最初のアクセスであれば、ステップS2へ進み、一連番号管理部12を呼び出し、要求に対してユニークな一連番号を付与する。その後、ステップS6へ進む。

【0029】初期アクセスでなければ、ステップS3へ進み、C o o k i e検証部14を呼び出して、C o o k i eが改ざんされたものでないかをチェックする。また、C o o k i eがコピーされたものでないかどうか併せてチェックする。この不正コピーのチェックは、例えばC o o k i eから抽出した一連番号とゲーム識別子(次地域番号)の組をその都度記録しておき、同一の一連番号とゲーム識別子の組が既に記録されているかどうかを調べるにより行うことができる。

【0030】ステップS4の判定により、C o o k i eが改ざんまたはコピーされたものである場合には、ステップS5へ進み、サービスを中止する。検証がOKであれば、ステップS6によりC o o k i e生成部13を呼び出してC o o k i eを生成する。続いてステップS7によりサービスのためのHTMLファイルを編集し、C o o k i eとHTMLファイルを要求元の利用者端末2へ送付する。

【0031】図4は、図1に示す一連番号管理部12の処理フローチャートである。一連番号管理部12は、サービスプログラム11から呼び出されると、まずステップS11により、一連番号最大値管理ファイル18に読み書きの競合防止のためのロックをかける。次に、ステップS12では、一連番号最大値管理ファイル18から現在記憶している一連番号の最大値を読み出す。ステップS13では、読み出した一連番号に1をプラスし、ス

テップS14により、その値を一連番号最大値管理ファイル18に書き戻す。次に、ステップS15では、一連番号最大値管理ファイル18の読み書き競合防止のロックを解除し、サービスプログラム11に一連番号を通知して処理を終了する。

【0032】図5(A)は、図1に示すCookie生成部13の処理フローチャートである。Cookie生成部13は、サービスプログラム11からのCookie生成要求により、まずステップS21においてCookie化対象データを1データ構造に編集する。次に、

ステップS22では、署名作成・検証部15を呼び出し、Cookie化対象データのデータ構造に対してデジタル署名を作成する。続いてステップS23では、Cookie化対象データのデータ構造とデジタル署名とを合成して、暗号化・復号化部16により暗号化し、その結果を送付するCookieとする。

【0033】図5(B)は、図1に示すCookie検証部14の処理フローチャートである。Cookie検証部14は、サービスプログラム11からのCookie検証要求により、まずステップS31において利用者

端末2から受け取ったCookieを暗号化・復号化部16によって復号する。ステップS32では、復号した結果のCookie化対象データのデータ構造とデジタル署名を抽出し、ステップS33により、デジタル署名が正当であるかどうかを検証する。ステップS34により、検証結果を判定し、検証結果がOKであれば、

ステップS35により検証OKのリターンコードを設定して、サービスプログラム11に検証成功を報告する。検証結果がNGであれば、ステップS36により検証NGのリターンコードを設定し、サービスプログラム11に検証失敗を報告する。

【0034】なお、サービスプログラム11では、この復号したCookieについてデジタル署名による検証のほか、要求ごとに一意に付与した一連番号により重複要求であるかどうかなどの検証を行う。

【0035】

【発明の効果】以上説明したように、本発明によれば、

利用者へのサービス提供の遷移をCookieにより制御するWWWサービスの提供において、利用者によるCookieの改ざんおよびCookieのコピーによるサービスの正常な実施への妨害を、Cookieにデジタル署名を付加することによりサービスを提供する計算機において検出することが可能になり、さらに暗号技術を用いてCookieのデータ構造を隠蔽し、デジタル署名および暗号化に用いる鍵をサービスを提供する計算機にのみ保持することによって、高いセキュリティでWWWサービスを提供することができるようになる。

【図面の簡単な説明】

【図1】本発明を実施するシステムの構成例を示す図である。

【図2】本発明の一実施形態の作用を説明するための図である。

【図3】サービスプログラムの処理フローチャートである。

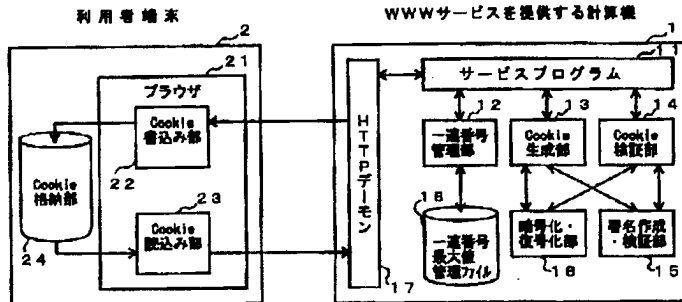
【図4】一連番号管理部の処理フローチャートである。

【図5】Cookie生成部とCookie検証部の処理フローチャートである。

【符号の説明】

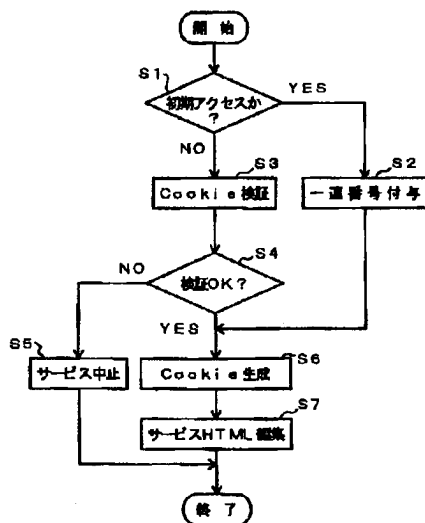
- 1 WWWサービスを提供する計算機
- 11 サービスプログラム
- 12 一連番号管理部
- 13 Cookie生成部
- 14 Cookie検証部
- 15 署名作成・検証部
- 16 暗号化・復号化部
- 17 HTTPデーモン
- 18 一連番号最大値管理ファイル
- 2 利用者端末
- 21 ブラウザ
- 22 Cookie書込み部
- 23 Cookie読込み部
- 24 Cookie格納部
- 3 Cookie

【図1】



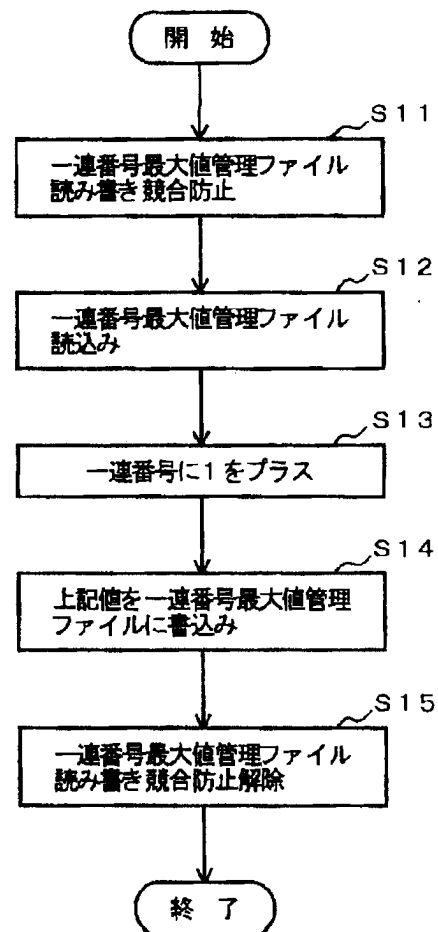
【図3】

サービスプログラムの処理フローチャート

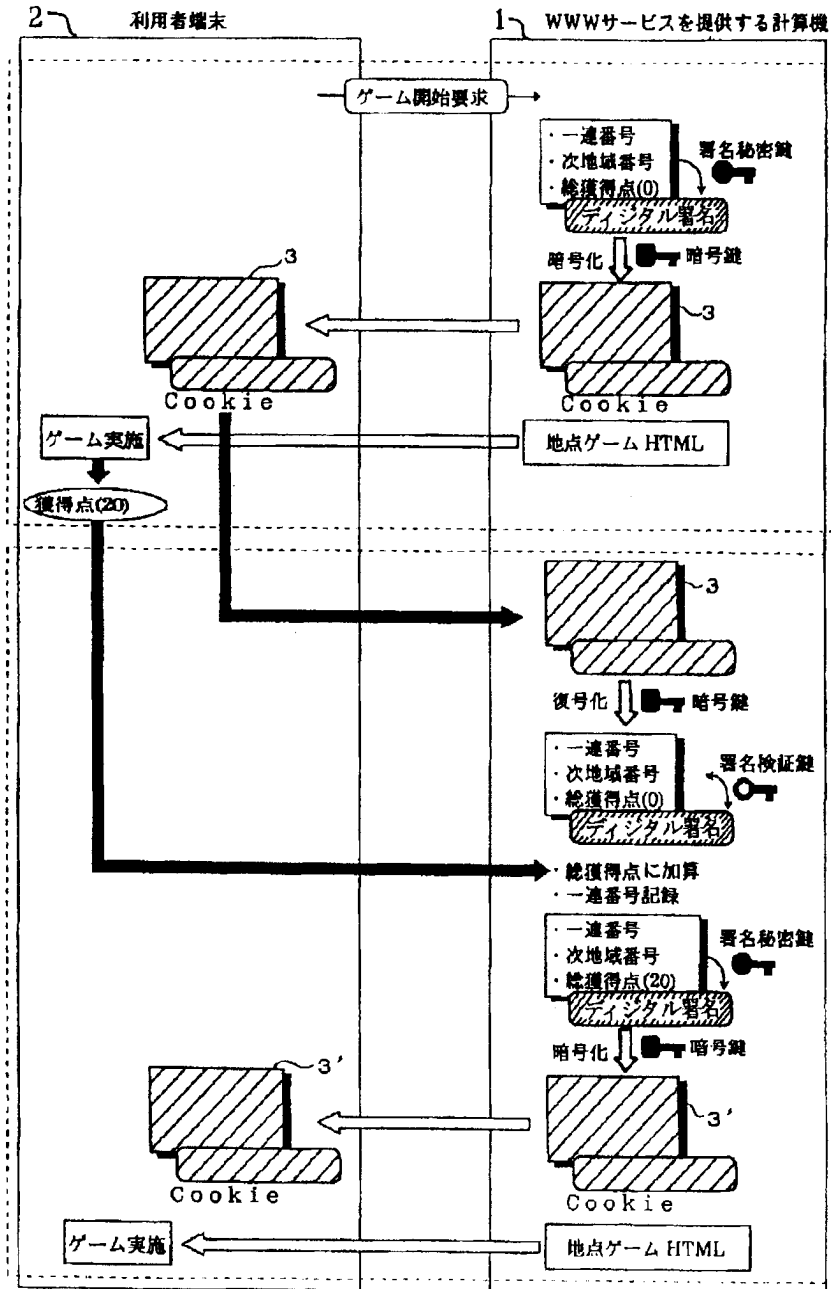


【図4】

一連番号管理部の処理フローチャート

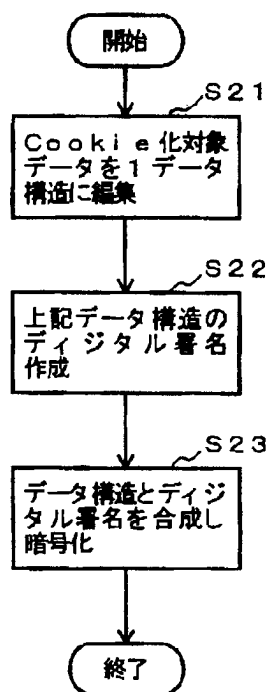


【図2】

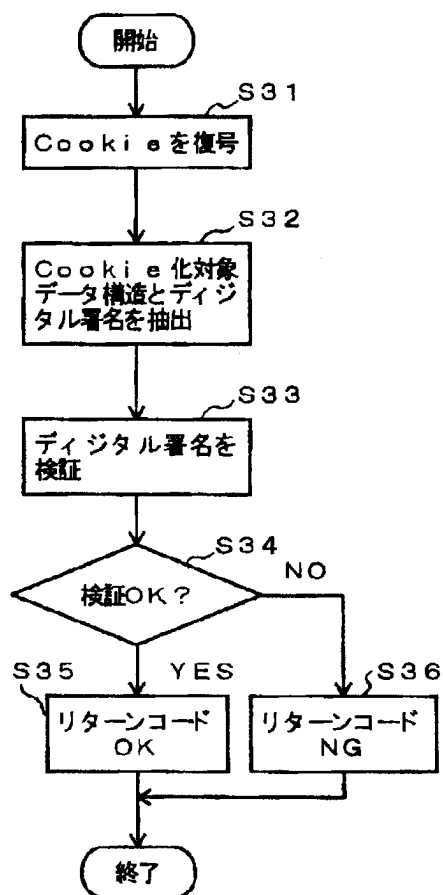


【図5】

(A) Cookie生成部



(B) Cookie検証部



フロントページの続き

(72)発明者 浅沼 透

東京都武蔵野市御殿山一丁目1番3号 エ
ヌ・ティ・ティ・アドバンステクノロジー株
式会社内